(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平8－340331

(43)公開日　平成８年(1996)12月24日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ　9/32			Ｈ０４Ｌ	9/00	６７３Ｂ
Ｇ０６Ｆ　15/00	３３０	9364－5L	Ｇ０６Ｆ	15/00	３３０Ｃ
Ｇ０９Ｃ　1/00	６４０	7259－5J	Ｇ０９Ｃ	1/00	６４０
			Ｈ０４Ｌ	9/00	６７３Ｃ

審査請求　未請求　請求項の数７　ＯＬ　（全９頁）

(21)出願番号　特願平8－131694

(22)出願日　平成８年(1996)５月27日

(31)優先権主張番号　４５５６１４

(32)優先日　1995年５月31日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　390035493
エイ・ティ・アンド・ティ・コーポレーション
ＡＴ&Ｔ　ＣＯＲＰ.
アメリカ合衆国　10013－2412　ニューヨーク　ニューヨーク　アヴェニュー　オブ　ジ　アメリカズ　32

(72)発明者　マイラ　エル．エンサー
アメリカ合衆国，07901　ニュージャージー，サミット，ビーチ　スプリング　ドライブ　３シー

(74)代理人　弁理士　三俣　弘文

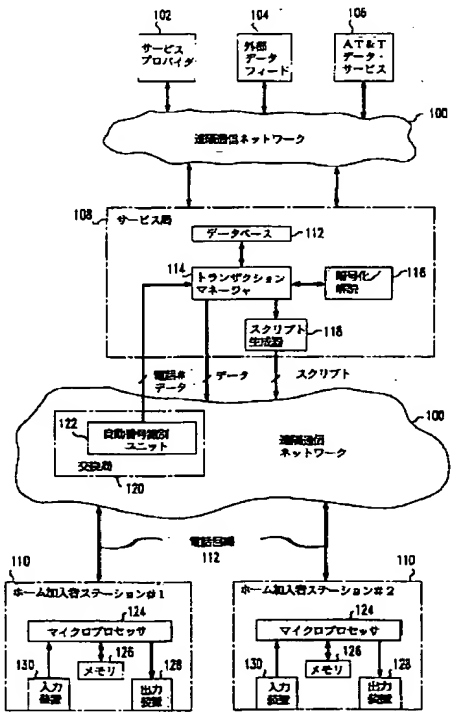
最終頁に続く

(54)【発明の名称】　ネットワークへのユーザ端末のアクセスを認証するための方法および装置

(57)【要約】

【課題】　複数の加入者ステーション１１０が通信可能に結合されたネットワーク１００のためのパスワード認証セキュリティーシステムを提供する。

【解決手段】　加入者ステーション１１０との通信の確立により、加入者ステーションが結合されている回線の電話番号を含むネットワーク結合識別子が、電話交換局１２０において検出され、制御センター１０８に送信される。１回目に通信が確立された場合、受信された電話番号は、秘密のパスワードを生成するために暗号化され、メモリ１２６に記憶させるために、加入者ステーション１１０に自動的に送信される。その後の通信において、電話番号が制御センター１０８により再度受信され、暗号化され、第２のパスワードが生成される。第１のパスワードが、ユーザとのかかわり合いと独立に、メモリ１２６から自動的に検索される。２つのパスワードが比較され、少なくとも類似している場合、制御センターが、加入者ステーションからの呼びをネットワークのサービスプロバイダ１０２、データベース１０４、１０６などに結合する。



1

【特許請求の範囲】

【請求項１】　有線ネットワーク、無線ネットワーク、衛星ネットワーク、ファイバ光ケーブルネットワーク、および同軸ケーブルネットワークのうちの１つからなる遠隔通信ネットワーク（１００）への、このネットワークと通信可能に結合された複数のユーザ端末（１１０）のうちの選択された１つからのアクセスに権限が与えられているかどうかを決定するための方法において、

選択されたユーザ端末から前記ネットワークへ入ってくる呼びの受信により、選択されたユーザ端末のネットワーク結合識別子を検出するステップと、

前記ユーザ端末からパスワードを受信するステップと、

前記識別子とパスワードを比較するステップと、

前記識別子の少なくとも一部が前記パスワードの少なくとも一部と一致する場合、前記ネットワークへのアクセスを前記選択されたユーザ端末に対して許可するステップと、

前記識別子および前記パスワードに一致する部分がない場合、前記ネットワークへのアクセスを前記選択されたユーザ端末に対して拒否するステップとを有し、

前記識別子が、選択されたユーザ端末から入ってくる呼びにより使用される前記ネットワークの通信チャネル（１１２）に関する情報を含むことを特徴とするネットワークへのユーザ端末のアクセスを認証するための方法。

【請求項２】　前記ネットワークが、前記ネットワークと通信可能に結合された、複数のユーザ端末から入ってくる呼びを受信するためのネットワークサービスセンターを有する電話ネットワークからなり、

ネットワーク結合識別子を検出するステップが、

電話ネットワーク交換局の自動番号識別ユニットから、選択されたユーザ端末の入ってくる呼びに結び付けられた電話番号を受信するステップであることを特徴とする請求項１記載の方法。

【請求項３】　ネットワークへのアクセスを許可するステップおよびネットワークへのアクセスを拒否するステップが、

識別子およびパスワードの少なくとも一部が一致する場合、選択されたユーザ端末の入ってくる呼びを、ネットワークサービス、ネットワークデータベース、およびネットワーク出力装置のうちの１つに結合するステップと、

識別子およびパスワードの少なくとも一部が一致しない場合、選択されたユーザ端末の入ってくる呼びを、ネットワークから切り離すステップであることを特徴とする請求項２記載の方法。

【請求項４】　ネットワークとユーザ端末との間に最初の通信が確立した場合に、

第１の暗号化されたパスワードを生成するために、識別子を暗号化するステップと、

2

前記ユーザ端末のメモリ中に記憶させるために、前記ネットワークを介して前記ユーザ端末へ前記第１の暗号化されたパスワードを送信するステップとをさらに有することを特徴とする請求項１記載の方法。

【請求項５】　識別子およびパスワードを比較するステップが、

ユーザ端末から受信された第１の暗号化されたパスワードとの比較のために、第２の暗号化されたパスワードを生成するために識別子を暗号化するステップと、検出された識別子との比較のために、解読された識別子を生成するために第１の暗号化されたパスワードを解読するステップとからなるステップから選択されたステップをさらに有することを特徴とする請求項１記載の方法。

【請求項６】　ネットワークに結合された複数のユーザ端末のうちの選択された１つからの前記ネットワークへのアクセスを認証するためのセキュリティーシステムにおける、前記ネットワークへのアクセスを得るために使用されるパスワードを選択し、前記選択されたユーザ端末に渡すための方法において、

ネットワークとユーザ端末との間の通信の確立に応じて、選択されたユーザ端末の通信チャネルおよびネットワークアドレスのうちの１つを検出するステップと、

秘密のパスワードを生成するために前記識別子を暗号化するステップと、

前記ネットワークを介して、ユーザ端末へパスワードを送信するステップとを有し、

前記識別子が、ネットワークへのユーザ端末の結合の固有の情報を含むことを特徴とするネットワークへのユーザ端末のアクセスを認証するための方法。

【請求項７】　ネットワーク（１００）に通信可能に結合された複数のユーザ端末（１１０）を有する遠隔通信ネットワークのためのセキュリティーシステムにおける、メモリ（１２６）を有する複数のユーザ端末のうちの選択された１つからネットワークへのアクセスを認証するための装置において、

ネットワークとユーザ端末との間の通信の確立に応じて、ネットワークに通信可能に結合された、選択されたユーザ端末のメモリからネットワーク結合識別子を受信するためのネットワークサービスセンター（１０８）を有し、

このネットワークサービスセンターが、

前記識別子と、選択されたユーザ端末のメモリ中の所定のロケーションから読み込んだパスワードとを比較するための比較ロジックと、

前記比較結果に基づいて、選択されたユーザ端末がネットワークへのアクセスを許可または拒否するためのスイッチとを含み、

識別子は、選択されたユーザ端末から入ってくる通信の通信チャネルインジケータ、ネットワークアドレス、および電話番号のうちの１つを含むことを特徴とするネッ

トワークへのユーザ端末のアクセスを認証するための装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、コンピュータネットワークおよび遠隔通信ネットワークの両者において使用されるパスワード認証セキュリティーシステムに関する。

【０００２】

【従来技術の説明】ネットワークセキュリティーは、ネットワークおよびネットワーク利用における最近の急増とともに、ますます問題となってきている。よりユーザフレンドリーなネットワークプラットフォームの出現および無数のオンラインデータベースおよびサービスへの容易なアクセスによって、伝統的な形のネットワークセキュリティーは、権限を与えられたユーザまたは支払っている加入者のみが守られたネットワークへのアクセスを得ることを可能にすることを保証するにはもはや十分ではなくなっている。

【０００３】ＵＮＩＸ™に基づくシステムのような典型的なコンピュータネットワークにおいて、セキュリティーは、ユーザログインおよび秘密のパスワードにより、各ユーザとセキュリティーチェックを実行するネットワークサーバとの間で遂行される。最初のアクセスにより、ユーザは、ネットワーク上の彼のアドレスとして使用されるべきログインと、認証のチェックに使用するための秘密のパスワードを選択する。ユーザは、これらの選択をネットワークサーバに送信し、秘密のパスワードは、暗号化されたデータベースすなわち彼のログインに結び付けられたディレクトリに格納される。

【０００４】その後のネットワークへの接続において、ユーザは、彼のログインおよび彼の秘密のパスワードの両者を質問される。サーバは、彼のログインを使用して、格納されたパスワードを検索し、それをユーザにより現在与えられているパスワードと比較する。認証チェックが実行され、両方のパスワードが同じ場合に、ユーザがネットワークへアクセスすることが許可される。

【０００５】

【発明が解決しようとする課題】しかし、この形のパスワードセキュリティーは、ユーザのかかわり合い依存する問題に悩まされている。ユーザは、まず、パスワードの選択または同意をすることを求められ、次に、パスワードを記憶し、ネットワークへアクセスすることを望むたびにサーバにパスワードを与えることを求められる。このようにする場合、多くのユーザーは、パスワードを忘れないように書きとめてあり、さらに、パスワードの入力を他人に知られないように実行することを必ずしもいない。

【０００６】従って、セキュリティーが、ネットワークに対して形成される特定の接続ではなく特定のユーザの

パスワードに依存しているので、この権限が与えられていないアクセスは、ネットワークに接続されているどの端末からも実行可能である。

【０００７】ネットワークユーザが、ホームバンキングおよびホームショッピングのような金融および消費者サービスに対する数百万人のネットワークユーザのうちの１人となる未来の世界において、このセキュリティーシステムが被害を受けやすいことは、さらに重大な事柄となる。数百万人の加入者それぞれについての加入者の財政の安全が各加入者の適切な行為に依存する場合、パスワードの秘密を維持する上で適切な手段をとらない加入者を容易にだます犯罪的構成要素が確かにある。また、選択されたパスワードは端末を特定するものではなく、ユーザを特定するものなので、加入者への口座またはサービスへの権限が与えられていないアクセスは、事実上知られることなく行うことができる。これは、違反者が特定の端末からアクセスを行うように制限されないからである。

【０００８】本発明の１つの目的は、ネットワークユーザまたは加入者に独立かつトランスペアレントなコンピュータネットワークまたは遠隔通信ネットワークのいずれかにおいてセキュリティーを遂行するための方法および装置を提供することである。

【０００９】本発明の他の１つの目的は、ユーザまたは加入者によりなされるネットワークへの特定の接続を識別するパスワードの認証に基づいて、ネットワークのサービス、データベースまたは装置へのアクセスを安全にするための方法および装置を提供することである。

【００１０】本発明のさらなる他の１つの目的は、ネットワークの自動番号識別サービスを使用することにより、パスワードが最初に生成され、その後に、ネットワーク制御センターにより自動的に認証される、電話ネットワークへのアクセスを安全にするためのパスワードセキュリティーシステムを提供することである。

【００１１】

【課題を解決するための手段】本発明は、自動的に決定されるネットワーク結合識別子および自動的に受信される暗号化されたパスワードに基づく、遠隔通信ネットワークまたはコンピュータネットワークのサービス、データベースまたは装置へのアクセスを安全にするための方法および装置を提供する。ユーザ端末または加入者ステーションからネットワークへアクセスがなされる場合、ネットワーク上でセキュリティーシステムを具現化するネットワーク制御センターは、ネットワークへの結合を特定するユーザ端末の固有のネットワーク結合識別子を、ネットワークから受信する。

【００１２】本発明の一実施形態において、ネットワークは、電話ネットワークであり、識別子は、ユーザ端末をネットワークへ結合する特定の電話回線の電話番号およびネットワークの自動番号識別サービスにより決定さ

れる番号で形成される。他の一実施形態において、ネットワークは、コンピュータネットワークであり、識別子は、特定の端末のネットワークアドレス、サーバ、またはユーザディレクトリで形成される。

【００１３】ネットワークへのユーザ端末の識別された結合により、ネットワークへの１回目のアクセスがなされた場合、ネットワーク制御センターは、秘密の暗号化されたパスワードを得るために、ネットワーク結合子を検出し、選択し、ネットワークに内在する暗号化キーを使用して暗号化する。そして、パスワードは、ユーザに知られないように、ユーザ端末のメモリ中にダウンロードされる。

【００１４】その後のユーザ端末によるネットワークへの各接続において、制御センターは、加入者の現在検出されているネットワーク結合識別子および同じネットワーク暗号化キーを使用して、もう１つの暗号化されたパスワードを生成する。次に、制御センターは、ユーザ端末のメモリに以前に格納された暗号化されたパスワードをアップロードし、この２つのパスワードを比較する。これらが一致する場合、これは、同じユーザ端末が同じネットワーク接続からアクセスを要求していることを意味し、いかなるユーザの干渉とも独立にセキュリティーが維持される。２つのパスワードが一致しない場合、ユーザに問題が通知され、パスワードまたはネットワークへのユーザ端末の結合のいずれかが偽造されたとみなして、ネットワーク接続がネットワーク制御センターにより終了される。

【００１５】

【発明の実施の形態】本発明は、複数のユーザ端末１１０、２０２を有するネットワーク１００、２００のためのパスワード認証セキュリティーシステムを提供する。複数のユーザ端末１１０、２０２は、ネットワーク１００、２００と通信できるように結合されている。図１および図２にそれぞれ示されているように、システムは、ネットワーク制御センター１０８、２０６をそれぞれ有する遠隔通信ネットワーク１００またはコンピュータネットワーク２００のいずれかにおいて具現化することができる。

【００１６】ネットワーク制御センター１０８、２０６は、ユーザ端末１１０、２０２によるネットワーク１１０、２００へのアクセスおよび通信を監視および／または処理するために、ネットワーク１００、２００に結合されている。ユーザ端末１１０、２０２は、割り当てられたデータ通信チャネル、ネットワークノードまたは遠隔端末リンクのアドレス、または電話ネットワークの電話回線のような固有に識別可能なネットワーク結合１１２、２１２を介して、ネットワーク１００、２００へ結合されている。

【００１７】図２に示されたコンピュータネットワーク２００において、ネットワーク制御センターは、ネットワークサーバ２０６および結び付けられたネットワークデータベース２０８からなる。ネットワークサーバ２０６および結び付けられたネットワークデータベース２０８は、ＬＡＮまたはＷＡＮのようなコンピュータネットワーク２００を介して複数のユーザ端末２０２およびネットワーク出力装置２０４に結合されている。コンピュータネットワーク２００へのアクセスは、典型的には、図示されていないネットワークサーバのアクセス制御ユニットにより監視され、実行される。

【００１８】コンピュータネットワーク２００への接続がユーザにより要求された場合、アクセス制御ユニットは、ユーザ端末２０２のネットワークアドレスすなわちロケーションを認知する。このロケーションは、そのローカルネットワークサーバアドレス、サブネットへの遠隔リンクアドレス、およびユーザの割り当てられたネットワークディレクトリを含み得る。制御ユニットは、ネットワークサーバ２０６への接続スロットの利用可能性を決定し、ユーザがネットワーク出力装置２０４および／またはネットワークデータベース２０８をアクセスするための権限を有するかどうかを決定する。

【００１９】図１において、有線ネットワーク、無線ネットワーク、衛星ネットワーク、ファイバ光ケーブルネットワーク、同軸ケーブルネットワークなどのような遠隔通信ネットワーク１００は、ネットワークサービス局を形成するネットワーク制御センター１０８を有するものとして示されている。ネットワークサービス局（ネットワーク制御センター）１０８は、ホームまたはビジネス加入者ステーションを形成する複数のユーザ端末１１０に結合されており、遠隔通信ネットワーク１００を介して、サービスプロバイダ・ステーション１０２、外部データフィード１０４、および外部データベース１０６に結合されている。

【００２０】この実施形態において、ネットワークサービス局１０８は、サービスプロバイダ・ステーション１０２からのオンラインサービスと外部データフィード１０４および外部データベース１０６からのデータとをホームおよびビジネス加入者ステーション１１０中の端末装置へ与えるための中間的送信ステーションとして働く。これを達成するために、ネットワークサービス局１０８は、ネットワーク接続、ネットワークパスワード認証、加入者ステーション１１０へのデータ通信およびスクリプト・メッセージングを処理するために、トランザクション・マネージャのようなマイクロプロセッサ・ロジック１１４、内部データベース１１２、およびスクリプト生成器１１８を含む。

【００２１】また、ネットワークサービス局１０８は、新たなハードウエア特徴および／またはサービスを具現化するために端末ソフトウエアをアップグレードするために、および端末に内在する新たなソフトウエアアプリケーションを提供するために、加入者ステーション１１

０の端末へのソフトウエアのダウンロードを可能にする。以下に説明する加入者装置の実施形態において、端末に内在する特定のソフトウエアが、端末に直接またはホームネットワークを介して結合され得る他の装置の動作を制御および処理するために、ライセンスされ、かつネットワークサービス局１０８から端末へダウンロードされ得る。

【００２２】そのような用途における本発明の１つの利点は、加入者端末を有するが特定のサービスについて登録されていないユーザが、他の登録されたユーザのネットワーク接続（すなわち、電話回線）を介して、登録されたユーザのネットワーク接続へ自分の端末を接続することにより、ソフトウエアを不正にダウンロードすることを防止することである。一度ダウンロードされたソフトウエアの不正な複製行為は、加入者端末が、コンピュータシステムである必要はないという事実により、ソフトウエアがそれによって複製される代替的入出力装置（すなわちフロッピー・ドライブ）を有さないようにすることにより禁止される。

【００２３】加入者ステーション１１０は、実際に、通常の方法により遠隔通信ネットワーク１００に接続されるように適合された、データの処理およびネットワークトランザクションの処理のためのマイクロプロセッサ１２４と、図示しないデータを送受信するトランシーバと、非持久性および／または持久性のデータ記憶のためのメモリ１２６と、ユーザからの入力を直接受け取るユーザ入力装置（すなわち、キーボード、マウス、リモコンなど）１３０と、メッセージおよびデータをユーザに対して表示するためのユーザ出力装置（すなわち、ディスプレイ、オーディオスピーカなど）１２８とを有するいかなる端末装置も含むことができる。このような端末装置（加入者ステーション）１１０は、電話ハンドセット、電話応答システム、およびコンピュータシステムを含み、これらに限定されない。

【００２４】図示されていないホーム加入者ステーションのための端末装置１１０の特定の例において、ホーム電話応答システムは、標準的オーディオ／ビデオ入出力を介してテレビジョンに結合され、標準的ＲＦ入出力を介してケーブルチャネルチューナーに結合され、標準的ＲＪ１１電話ジャックを介して電話ネットワークに結合される。

【００２５】このシステムは、入力装置としてのリモコン、出力装置としてのテレビジョンディスプレイモニタを有し、さらに、ネットワークトランザクションの処理およびデータの処理のためのメモリを有するマイクロプロセッサと、入ってくる呼びおよび出ていく呼びを処理するための呼び信号演算処理ユニットと、デジタル信号を処理し、ＤＴＭＦトーンを検出し、マイクロプロセッサへ情報を通知し、デジタル応答マシンおよびデータモデムを具現化するために呼び信号演算処理ユニットと相互作用するデジタル信号演算処理ユニットと、リモコン、ケーブルチャネルチューナー、およびテレビジョンモニタの間で信号を受信し、処理し、送信するためのビデオ変調器／エンコーダユニットを含む。

【００２６】上述の実施形態において、加入者とネットワークサービス局１０８との間の典型的なトランザクションは、加入者ステーションの端末装置１１０にネットワークサービス局１０８への通話を開始するように指示する加入者からなる。これは、ユーザ端末を立ち上げて、端末ディスプレイ１２８上に生成されるメニュ選択から「オンラインサービス」オプションおよび「ソフトウエアダウンロード」オプションのうちの１つを選ぶことにより達成される。次にユーザ端末は、ネットワークサービス局１０８へのモデム通話を開始し、モデムハンドシェイクが完了した後、自動ユーザトランスペアレント認証ハンドシェイクが開始される。

【００２７】図３のフローチャートに示されているように、認証ハンドシェイクは、サービス局トランザクションマネージャ１１４（図１）により、ネットワークサービス局１０８によりユーザ端末へのアクセスを得ようとする特定のユーザ端末１１０のための固有のネットワーク結合識別子を遠隔通信ネットワーク１００からまず受信することにより実行される。通常の電話ネットワーク（遠隔通信ネットワーク）１００の場合、この識別子は、ユーザ端末１１０を遠隔通信ネットワーク１００に結合する専用の電話回線に結び付けられた電話番号からなる。

【００２８】この電話番号は、例えば、接続された電話ネットワーク交換局１２０内で使用される自動番号識別ユニットすなわちサービス１２２による番号の検出により、通常の方法で得られる。しかし、なんらかの理由で、自動番号識別サービス１２２が端末の電話番号を提供しない場合、サービス局トランザクションマネージャ１１４は、結び付けられた入力装置１３０の使用により電話番号を直接提供するように加入者に要求するユーザ端末１１０へ、スクリプトメッセージをダウンロードする。

【００２９】特定のユーザ端末１１０の電話番号が受信されると、サービス局トランザクションマネージャ１１４は、この番号をネットワークサービス局１０８の暗号化／解読ユニット１１６へ送る。この番号は、図示しない通常の暗号生成器を使用して暗号化され、秘密の暗号化されたパスワードが生成される。次に、サービス局トランザクションマネージャ１１４は、そのロケーションに以前に格納されたであろうパスワードをメモリ１２６の所定のロケーションから検索することを、ユーザ端末１１０の端末マイクロプロセッサ１２４に要求する。

【００３０】このメモリロケーションにパスワードが発見されなかった場合、端末マイクロプロセッサ１２４は、この状態をサービス局トランザクションマネージャ

１１４に通知し、サービス局トランザクションマネージャ１１４は、特定のユーザ端末１１０がすでにネットワークサービス局１０８により登録されているかどうかを決定するために、ネットワークサービス局の内部データベース１１２に質問する。これは、暗号化されたパスワードを、ネットワークサービス局の内部データベース１１２に格納された全てのユーザ端末１１０の登録された口座を識別するために使用される暗号化されたパスワードのリストと比較することにより行われる。

【００３１】この比較において、暗号化されたパスワード間の一致が見いだされなかった場合、これは、ユーザ端末１１０が以前に登録されていなかったことを意味する。従って、サービス局トランザクションマネージャ１１４は、新たに暗号化されたパスワードにより識別された内部データベース１１２中に加入者登録口座をつくることにより、この特定のユーザ端末を登録する。また、１１４は、新たに暗号化されたパスワードをメモリ１２６の所定のロケーションに記憶させるためにユーザ端末１１０に送信する。その後の認証ハンドシェイクにより、ユーザ端末１１０は、以前に登録されていたと決定されることになる。

【００３２】最後に、ネットワークサービス局１０８は、要求されたソフトウエアをユーザ端末１１０にダウンロードすることにより、またはユーザ端末１１０をサービスプロバイダ１０２に結合することにより、トランザクションを続ける。サービスプロバイダ１０２への結合は、入ってくる呼びをサービスプロバイダ１０２に送る（または、リレーする）こと、またはサービスプロバイダの電話番号をユーザ端末に提供することのいずれかにより、実行される。そして、その後の呼びにより、直接的な接続が形成できるようになる。

【００３３】しかし、新たに暗号化されたパスワードと暗号化されたパスワードのデータベースリストとが一致する場合、これは、端末のメモリ１２６中にあったはずのパスワードが偽造されたか、またはメモリ１２６からのパスワードの読みだしあるいはネットワークサービス局１０８へのパスワードの送信においてハードウエア故障があったかのいずれかを意味する。いずれの場合にも、エラーメッセージは端末の出力装置１２８に送られて、表示され、加入者に問題を通知し、この問題を解決するためにネットワークサービス局１０８への音声通話を行うよう加入者に指示する。そして、サービス局トランザクションマネージャ１１４は、加入者を遠隔通信ネットワーク１００から分離するために、モデム接続を終了させるよう遠隔通信ネットワーク１００に指示する。

【００３４】メモリ１２６中の所定のロケーション中に格納されたパスワードを検索するためのユーザ端末１１０へのトランザクションマネージャの要求がパスワードを返す場合、これは、ユーザ端末１１０が以前のトランザクションにおいてすでに登録されていたことを意味する。この場合、サービス局トランザクションマネージャ１１４は、新たに暗号化されたパスワードを認証目的のために検索されたパスワードと比較する。

【００３５】２つのパスワードが同一でない場合、エラーメッセージがユーザ端末１１０に送られ、端末のメモリ１２６に格納されたパスワードの偽造、ハードウエア故障、または特定のユーザ端末と専用の電話回線１１２との間のミスマッチのために、認証が失敗したことを加入者に対して表示する。再び、加入者は、問題を解決するためにネットワークサービス局１０８への音声通話をなすように指示され、モデム接続は終了される。

【００３６】２つのパスワードが同一であると決定された場合、認証ハンドシェイクは成功して、ネットワークサービス局１０８は、要求されたソフトウエアをユーザ端末にダウンロードすること、またはユーザ端末１１０を１０２に結合することにより、トランザクションを続ける。ネットワーク１００、２００へのアクセスを許可するかどうかを決定するために、パスワードの一致についての比較を実行することが好ましいが、パスワードが単に類似している場合、またはパスワードの一部のみが実際に一致している場合に、アクセスが許可されるパスワード比較を実行することも有利である。

【００３７】これは、例えば、ネットワークユーザの所定のグループ内の各ユーザへのアクセスを許可することが望ましい場合に有利となる。従って、コンピュータネットワーク２００について、これは、各ユーザのネットワークアドレスがサブネットワークを特定するという事実によって、所定のサブネットワーク上の全てのユーザがコンピュータネットワーク２００へのアクセスを得ることを可能にする。電話ネットワーク１００について、これは同様に、各加入者についての電話番号が同じ地理的トランク番号を含むという事実によって、特定の交換局によりサービスされる所定の地理的領域内の全ての加入者が電話ネットワーク１００へのアクセスを得ることを可能にする。

【００３８】また、ユーザ端末１１０、２０２のメモリ１２６内に格納されたパスワードを自動的に変更すること、および制御センターの内部データベース１１２、２０８中に格納されたパスワードの対応するリストを更新することのために、ネットワーク制御センター１０８、２０６においてプロセスを遂行することにより、この自動的ユーザトランスペアレント・パスワード認証システムをより信頼できるものとすることができることが予知される。これは、ネットワーク制御センター１０８、２０６により生成された異なる暗号化キーを使用してネットワーク結合識別子を暗号化することにより、選択されたユーザ端末１１０、２０２についての最初のパスワード認証の後に実行されることになる。

【００３９】ネットワーク制御センター１０８、２０６は、それ自体の内部データベース１１２、２０８および

11

ユーザ端末１１０、２０２の所定の（または代わりの）メモリロケーション１２６のそれぞれの中のオリジナルのパスワードをユーザの知識なしに自動的に置き換える。また、識別子が暗号化される場合、満了日をパスワードに追加し、ユーザがネットワークおよび／または特定のサービスに現在登録されているかどうかをサービスプロバイダに通知することができる。

【００４０】ここに記載された実施形態は、本発明の原理を開示するものであるが、これらの実施形態は、単なる例示であり、本発明の精神および範囲から離れることのない様々な付加および修正があり得る。例えば、ネットワークから加入者へのサービスおよび情報の提供のためのネットワークサービス局での加入者のトランザクションのシナリオにおいて、本発明は、ネットワークにより加入者の電話に割り当てられた電話番号を介して、サービス局において維持されている加入者口座をもつ加入者を固有に識別するために使用できる。加入者を異なる所在すなわち加入者ステーションに再割り当てすることができるが、加入者の古い電話番号の新しい加入者ステーションへの再割当は、サービス局が、再割当にもかかわらず、以前の口座との加入者の関連性を維持することを可能にする。

【００４１】

【発明の効果】以上述べたように、本発明によれば、ネットワークユーザまたは加入者に独立かつトランスペアレントなコンピュータネットワークまたは遠隔通信ネットワークにおいてセキュリティーを遂行するための方法および装置を提供することができる。

【図面の簡単な説明】

12

【図１】　複数の加入者ステーションがネットワークサービス局、複数のサービスプロバイダステーション、および複数のデータフィードおよびデータベースのそれぞれに結合される本発明の一実施形態による遠隔通信ネットワークを示すブロック図。

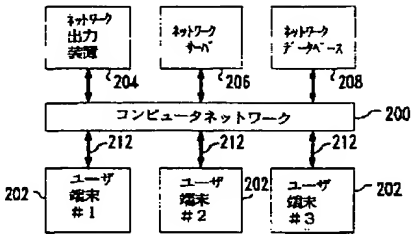
【図２】　複数のユーザ端末がネットワークサーバ、ネットワークデータベース、およびネットワーク出力装置に結合される本発明の一実施形態によるコンピュータネットワークを示すブロック図。

【図３】　本発明の一実施形態による遠隔通信ネットワークにおいて遂行されるパスワード認証プロセスを示すフローチャート。

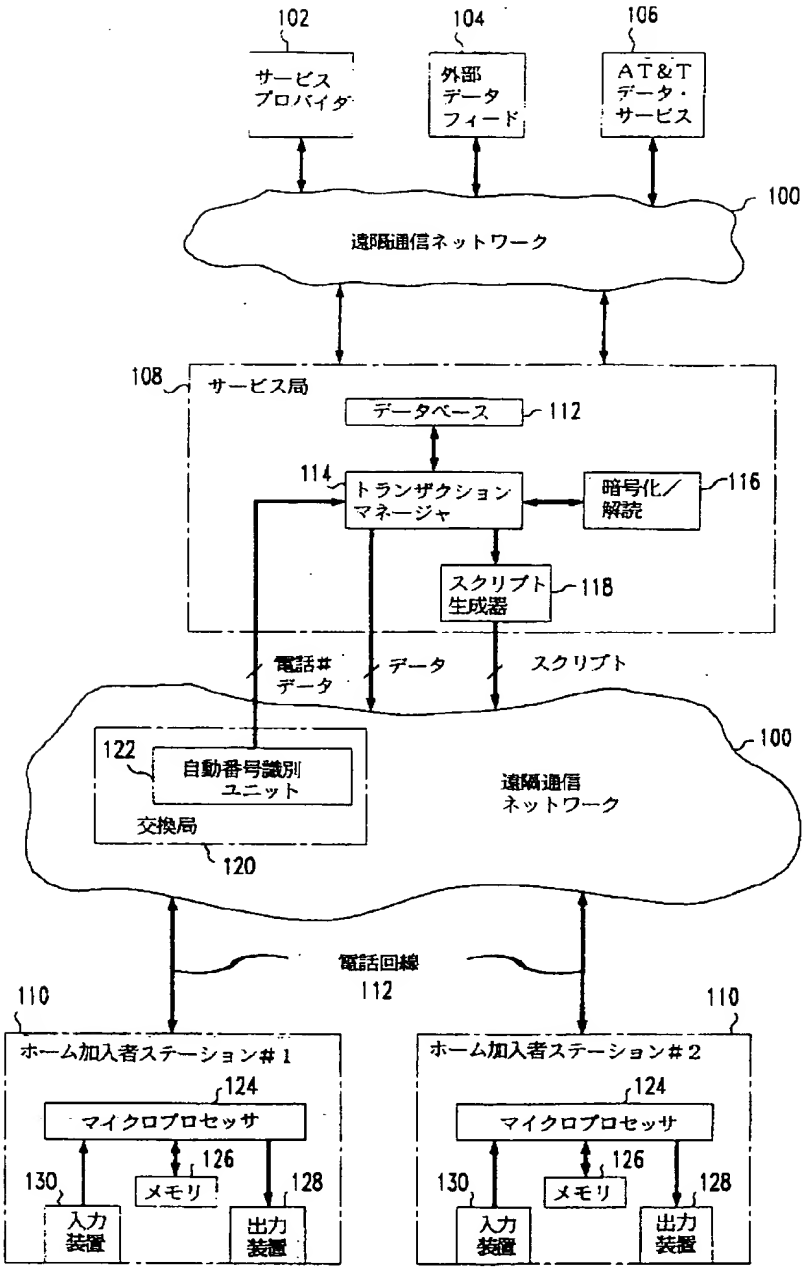
【符号の説明】

１００	遠隔通信ネットワーク
１０２	サービスプロバイダステーション
１０４	外部データフィード
１０６	外部データベース
１０８	ネットワーク制御センター（サービス局）
１１０	加入者ステーション
１１２	電話回線
１１４	トランザクションマネージャ
１１６	暗号化／解読ユニット
１１８	スクリプト生成器
１２０	電話ネットワーク交換局
１２２	自動番号識別ユニット
１２４	マイクロプロセッサ
１２６	メモリ
１２８	出力装置
１３０	入力装置

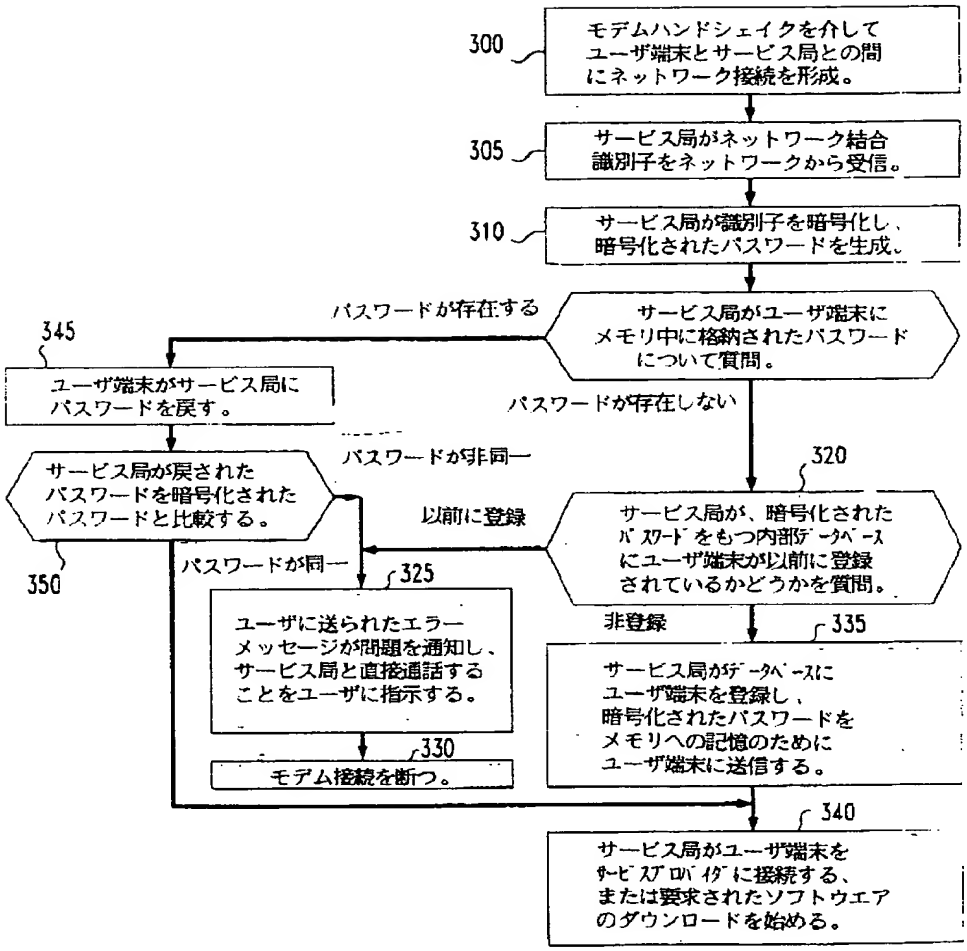
【図２】



【図１】


102
サービス
プロバイダ
104
外部
データ
フィード
106
AT&T
データ・
サービス
100
遠隔通信ネットワーク
108
サービス局
データベース
112
114
トランザクション
マネージャ
暗号化／
解読
116
スクリプト
生成器
118
電話#
データ
データ
スクリプト
122
自動番号識別
ユニット
交換局
120
100
遠隔通信
ネットワーク
電話回線
112
110
ホーム加入者ステーション#１
124
マイクロプロセッサ
126
メモリ
130
入力
装置
128
出力
装置
110
ホーム加入者ステーション#２
124
マイクロプロセッサ
126
メモリ
130
入力
装置
128
出力
装置

【図３】



フロントページの続き

(72)発明者　タッデュス　ジュリアス　コワルスキー
アメリカ合衆国，07901　ニュージャージー，サミット，ストーンリッジ　ロード　73

(72)発明者　アジェシノ　プリマティック
アメリカ合衆国，08825　ニュージャージー，フレンチタウン，ワゴン　ホイール　ドライブ　4

拒絶理由通知書

W 8 KY

特許出願の番号	特願２００１－１７６４１８
起案日	平成１７年　８月　４日
特許庁審査官	高橋　宣博　９３７４　５Ｊ００
特許出願人代理人	岡部　正夫（外１０名）　様
適用条文	第２９条第２項

この出願は、次の理由によって拒絶をすべきものである。これについて意見があれば、この通知書の発送の日から３か月以内に意見書を提出して下さい。

理　由

この出願の下記の請求項に係る発明は、その出願前日本国内又は外国において頒布された下記の刊行物に記載された発明又は電気通信回線を通じて公衆に利用可能となった発明に基いて、その出願前にその発明の属する技術の分野における通常の知識を有する者が容易に発明をすることができたものであるから、特許法第２９条第２項の規定により特許を受けることができない。

記　（引用文献等については引用文献等一覧参照）

・請求項　１－１２
・引用文献等　１－３
・備考

１．引用文献の記載事項

（１）引用文献１

「If the time run out, i.e. if the mobile terminal cannot authenticate itself at the access node within the predefined time period, then the already setup wireless ATM radio communication connection is interrupted (closed) and information regarding the mobile terminal (which has unsuccessfully attempted an authentication) is stored is the access node. Preferably, if the same mobile terminal has already failed an authentication a predetermined number of times, then further access requests from this mobile terminal are immediately rejected by the access node.」（第１２頁）と記載されており、認証失敗という結果になるときには、移動体ユニットのネットワークへのアクセスを拒絶する技術が示されている。

（２）引用文献２
「【００３５】２つのパスワードが同一でない場合、エラーメッセージがユーザ端末１１０に送られ、端末のメモリ１２６に格納されたパスワードの偽造、ハードウエア故障、または特定のユーザ端末と専用の電話回線１１２との間のミスマッチのために、認証が失敗したことを加入者に対して表示する。再び、加入者は、問題を解決するためにネットワークサービス局１０８への音声通話をなすように指示され、モデム接続は終了される。」と記載されており、認証が失敗した時にアナウンスメントを移動体ユニットに提供する技術（エラーメッセージがユーザ端末１１０に送られ）、及び、顧客サービスセンターに連絡する技術が示されている。

（３）引用文献３
「【０００５】
【発明が解決しようとする課題】ところで、上述した従来の電話端末装置では、メールの授受を行うために、サービスセンタへの発呼のための操作が必要となる。例えば、通信相手が発呼に応答しなかった場合、その発呼元の電話端末装置では、一旦通信相手への発呼を終了した後に、改めてサービスセンタに対する発呼を行わなければならない。つまり、発呼元の電話端末装置のユーザは、一旦発呼を終了するための操作と新たな発呼のための操作とを行う必要があり、そのために煩わしさを感じてしまう可能性がある。
【０００６】これに対して、周知の転送技術（転送電話サービス）等を利用して、通信相手への発呼をサービスセンタへの発呼に自動的に切り替えることも考えられる。」と記載されており、電話が繋がらない場合に、別の場所へ自動的にルーティングする技術が示されている。

２．判断
引用文献２に記載された認証失敗時の技術を引用文献１に適用することは当業者が容易になし得る。

引用文献２では、顧客サービスセンターへの連絡を改めて加入者が行うことになっているが、発呼先を切り替える必要性がある場合に、自動でルーティングする技術は引用文献３に示されており、引用文献２に引用文献３に記載された技術を適用することは当業者が容易になし得る。

拒絶の理由が新たに発見された場合には拒絶の理由が通知される。

引　用　文　献　等　一　覧
１.国際公開第９９／４４３８７号パンフレット

2.特開平０８－３４０３３１号公報

3.特開平１１－３３１４１２号公報

先行技術文献調査結果の記録

・調査した分野　ＩＰＣ第７版　Ｈ０４Ｂ７／２４－７／２６
Ｈ０４Ｑ７／００－７／３８

ＤＢ名

・先行技術文献

この先行技術文献調査結果の記録は、拒絶理由を構成するものではない。